CSO
FROM IDG

Ransomware
SURVIVAL GUIDE

From Stoned to pwned | *Attacks against businesses increased threefold in 2016* | **Ransomware-as-a-Service fuels explosive growth** | A fresh look at fighting ransomware | *Most victims able to thwart attacks, report says* | **Why you shouldn't pay the fee**

What you need to know about ransomware in 2017

In 2016, ransomware grew by every measure, from an increased rate of attacks to more variations and more new families, greater sophistication, and even a business model that allowed more criminals to take part.

While we don't expect the attackers to let up in the year ahead — they're making far too much money for that — the story of ransomware in 2017 is yet to be written, and there's plenty you can do to protect your organization.

One logical place to focus your energy is on user training at all levels, including the board. As Kaspersky Lab noted in a report on ransomware, last year "one in five cases involving significant data loss came about through employee carelessness or lack of awareness." We can do better.

In this guide from the editors of CSO, you'll learn:

- How ransomware is evolving and what that means for you
- Why effective user training is more important than ever
- What experts say you should do if the worst happens.

CONTENTS

3
From Stoned to pwned

5
Attacks against businesses increased threefold in 2016

7
Ransomware-as-a-Service fuels explosive growth

10
A fresh look at fighting ransomware

14
Most victims able to thwart attacks, report says

16
Why you shouldn't pay the fee

From Stoned to pwned

Beyond a sound backup strategy and software products like antivirus, your best defense is developing a keen eye for things that aren't what they appear to be.

BY DAVE LEWIS

When I was in the trenches as a defender I saw all manner of malicious software. The first I ever encountered back in the late 80s was the Stoned virus. This was a simple program that was lobbying the infected computer operator on the subject of legalizing marijuana. It was spread through infected floppy disks.

Years later I found myself standing in the office of one senior staff member who moonlighted as a university professor when he received an email from a student. The student professed her love for him and he was moved by the moment and clicked to open the email. I lurched forward in a vain attempt to stop him, but the damage was already done.

I had no idea what the email was, but I instinctively knew that it wasn't good. Much to our chagrin we discovered that this was the day that the Love Bug virus was unleashed on the internet. That was a long day.

Later in my career I found myself managing the antivirus system for an enterprise. When I rolled out a fresh enterprise deployment from $AVcompany I discovered that there were dozens of systems on the network that had either ancient installs of antivirus software or, in several cases, none at all. It was amazing that there had been a half-assed approach to managing the install base.

Flash forward to today. Malicious software has gone from being an abject annoyance to a criminal enterprise. Ransomware is the new vogue for online criminals. Why, because it is working for them. The concept is simple. A piece of malicious software infects a person's system and then encrypts files or, in some cases, the entire hard drive. Then a demand is posted to pay an amount of money via bitcoin to recover the files. Some have paid this ransom, which has fueled the resolve of the criminals, allowing the attacks to continue.

All is not lost for the infected victims. In many cases there are decryptor tools available for folks to rescue their files. This is possible in large part by the work of security researchers who have been able to reverse the malicious software. A noble endeavor.

How can you combat this sort of threat? Well, having a sound backup strategy is a strong first step. I have worked in many environments over the last twenty-five years and in some environments there was a backup process for some key servers and in only one did I find a backup plan for laptops and desktops.

If you have your files on your system backed up you will be able to recover in the event that your system is compromised. This doesn't mean you should run off and buy a removable hard drive and back up your work system. Engage with your IT department at the office. For a personal back up this helps, but be sure to encrypt it just in case it goes missing at some point.

Love it or hate it, having up-to-date malicious software defenses, like antivirus products, will help to reduce the risk. Of course this is not an ironclad guarantee by any stretch of the imagination, but it's better than a swift kick in the nethers.

The simple thing to remember: if you're not sure about something, do not click it. Received an invoice from a company you never heard of? Then it is likely it isn't what it appears to be. Also, be sure to keep a keen eye on the websites you are visiting. Is it CSOonline dot com or CSOnline dot com. Two very different results.

When we look at the trajectory of malicious software from the Stoned virus in the late 80s to the ransomware of today, we see that the annoyances of the past have become the tools of criminals today.

Ransomware attacks against businesses increased threefold in 2016

Kaspersky Lab recorded one ransomware attack every 40 seconds against companies in September.

BY LUCIAN CONSTANTIN

The number of ransomware attacks targeting companies increased threefold from January to September, affecting one in every five businesses worldwide.

According to a recent report from security company Kaspersky Lab, the rate of ransomware attacks against businesses increased from one every two minutes to one every 40 seconds during that period. For consumers it was even worse, with the rate reaching one attack every 10 seconds in September.

During the third quarter of the year, there were 32,091 new ransomware variations detected by Kaspersky Lab, compared to only 2,900 during the first quarter. Overall, 62 new ransomware families appeared this year, the company said.

This shows the interest that cybercriminals have in this type of malware and highlights its continued success, despite actions by law enforcement agencies and free decryption tools released by researchers and security companies.

Kaspersky's research revealed that small and medium-size businesses were hit the hardest, 42 percent of them falling victim to a ransomware attack over the past 12 months. Of those, one in three paid the ransom, but one in five never got their files back, despite paying.

Overall, 67 percent of companies affected by ransomware lost part or all of their corporate data and one in four victims spent several weeks trying to restore access, the Kaspersky researchers said.

The most successful ransomware program this year was CTB-Locker, accounting for 25 percent of all affected users. Next on the list was Locky with 7 percent and TeslaCrypt with 6.5 percent, even though this ransomware family was only active until May.

Ransomware attacks have become more targeted, with attackers crafting their spear-phishing and social engineering attacks for specific organizations or industry segments that are more likely to be affected by a lack of data availability.

Employee IT security training remains very important in preventing ransomware attacks. According to Kaspersky, one in five incidents that resulted in significant data loss were caused by employee carelessness or lack of security awareness.

Companies should back up data regularly, use reliable endpoint security solutions, keep the software installed on their systems up-to-date, restrict access to sensitive data and educate their employees and IT teams about ransomware risks.

If they become victims, companies should

check the No More Ransom website set up by security companies to check if there's a decryption tool available that could help them get their files back. They should also report incidents to their local law enforcement immediately, the Kaspersky researchers said.

The security vendor advises companies not to pay the ransom because this can make them an even bigger target and increases the chance that the next ransom will be higher. It also encourages cybercriminals and might not result in the recovery of the affected files.

Ransomware-as-a-Service fuels explosive growth

The best solutions are the preventive ones, and that means not only installing software patches and updates as soon as they become available, but educating users to become savvy enough not to fall victim to phishing emails.

BY TAYLOR ARMERDING

Believe it — you too can become a successful cybercriminal! It's easy! It's cheap! It's short hours for big bucks! No need to spend years on boring things like learning how to write code or develop software.

Just download our simple ransomware toolkit and we can have you up and running in hours — stealing hundreds or thousands of dollars from people in other countries, all from the comfort of your home office — or your parents' basement. Sit back and watch the bitcoin roll in!

OK, that's not the literal pitch coming from the developers of ransomware. But, given the rise of Ransomware as a Service (RaaS) — a business model in which malware authors enlist "distributors" to spread the infections and then take a cut of the profits — it sounds like it could be a candidate for the kind of "direct-response" TV ads that made the late pitchman Billy Mays famous.

As Trend Micro put it more soberly in a recent blog post, "Potential distributors don't even need much capital or technical expertise to start; even those without coding experience can launch a ransomware campaign." Indeed, the cost of some ransomware packages is less than $100.

In other words, just about anybody can do it.

All of which, until the recent ransomware attack on San Francisco's Municipal Transportation Agency, has seemed to be happening a bit under the radar.

With high-profile Distributed Denial of Service (DDoS) attacks like the one against internet backbone provider Dyn grabbing most of the recent headlines, you could be forgiven for thinking that ransomware might be on the decline.

But the reality is just the opposite, according to various experts and studies.

According to a white paper from Osterman Research, it is at "epidemic" levels, with nearly 50 percent of U.S. companies experiencing a ransomware attack during the past year.

And a Trend Micro report released in August found that about 80 new ransomware "families" — an increase of 172 percent — were discovered in the first half of 2016. A single, older version of the CryptoWall family brought in an estimated $325 million in 2015.

Ed Cabrera, chief cybersecurity officer at Trend Micro, said things have become markedly worse since that report. He said at the end of September, 2016, the increase was 400 percent. "In 2015, there had been 29 families observed, and as of September, we have observed and blocked 145 families," he said.

That is no surprise to Andrew Hay, CISO at DataGravity, who said a DDoS attack tends to get more publicity because, "it affects all users of a product or service, so the news of its impact spreads at the speed of typical internet news.

"Ransomware, conversely, is often hidden from people outside the company until the company, attacker or affected customers release details," he said.

Javvad Malik, security advocate at AlienVault, has a similar take on it. Many companies don't report ransomware attacks, he said, while DDoS attacks are, "by design, intended to be as publicly visible as possible."

But they agree, ransomware is a growth industry. "I don't think it has peaked. I think it is just getting started," said Christopher Hadnagy, chief human hacker at Social-Engineer. "I still hear of lots of accounts of companies left to either pay or start over."

And Orla Cox, director of security intelligence delivery at Symantec, said not only has the number of attacks increased, but the demanded ransom has as well.

"The average ransom demand has more than doubled, and is now $679 (U.S. dollars), up from $294 at the end of 2015," she said.

She added that 2016, "has also seen a new record in terms of ransom demands, with a threat known as 7ev3n-HONE$T (Trojan.Cryptolocker.AD)," which demands a ransom of 13 bitcoin per computer, or $5,083, at the time of discovery in January.

One reason for that explosive growth is probably because, even with headlines and continuous warnings about it, most individuals and organizations remain woefully vulnerable. Even if protection is available, they don't always use it.

The recent attack on the San Francisco MTA (known as "Muni") is an example. Security researcher and blogger Brian Krebs noted in a recent post that the attacker actually advised his victims to, "Read this and install patch before you connect your server to internet again," with a link to an advisory Oracle issued about a vulnerability in its Oracle WebLogic Server.

Oracle had made that patch available on Nov. 10, 2015 — more than a year ago.

Another reason for ransomware's success is that it takes time for security researchers to decrypt the files so they can provide solutions that will block them.

That work is ongoing. Malik said once researchers can break into the software, "they are able to create signatures or indicators of compromise."

A collaborative effort is by the Cyber Threat Alliance (CTA), founded by security vendors Fortinet, Intel Security, Palo Alto Networks and Symantec, which has used shared threat intelligence — in its words, "a huge effort of pooling the Alliance's collective resources," to track and analyze the CryptoWall family.

According to the alliance, the effort led to "enhanced protection against this threat with each member's individual products," plus building public awareness through its reports."

Other experts applaud sharing threat data, but note that it remains reactive — the updates, patches and other tools to block malware don't show up until after the threat has already caused plenty of damage.

Hay said antivirus and antimalware products are good at "protecting the low-hanging fruit," but the threats evolve too quickly for any tool to offer 100 percent protection.

He added that while he supports the goals of the CTA, "it is a members-only club. To join that club, you must provide a minimum of 1,000 unique malware executables daily that do not overlap with VirusTotal."

"This high barrier to entry means that while the goals of the alliance are good, it's simply not inclusive enough to help those affected," he said. "A better solution would be to open the doors and let vetted organizations and researchers contribute and work with the samples."

Cabrera called the sharing of threat information "critical to combating all cyber threats."

But he said the reality is that "due to the

dynamic nature of these threats, obtaining and sharing actionable intelligence in a timely manner is the biggest challenge."

He, like all experts, agreed that there is no "silver bullet" that will block all threats. But he said, "a layered, connected threat defense that protects endpoint, network and cloud infrastructure," will at least allow organizations to manage the ransomware threat.

The best solutions, however, are the preventive ones, which include:

- Install software patches and updates as soon as they are available.
- Become savvy enough not to fall victim to phishing emails. "Be wary of unexpected emails especially if they contain links and/or attachments," Cox said, adding that users should be especially careful of any Microsoft Office email attachment that advises enabling macros to view content. "Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros," she said.
- Do regular backups — and make sure those have added protection or are stored offline.

Hay said organizations can start by limiting access to their most important data and then rigorously monitor the network for anomalies.

"When these anomalies are detected, you can automatically create copies of your files in a safe location," he said, but added that it is also important to test the restoration of backups. "The last thing you want in the midst of an incident is to learn that your backups don't work," he said.

Finally, experts are mixed on the wisdom of paying the demanded ransom.

Hadnagy and Cox take the hard line. "Never," Hadnagy said. "Sadly many times even if the ransom is paid they do not unlock the files. It seems that if the ransom is paid the criminals learn it is good business and continue this type of attacks."

Cox agreed, for the same reasons — no guarantee that files will be unlocked, and increased likelihood of being attacked again.

Cabrera added that even if the attacker provides the encryption key, he could have already exfiltrated data that could be sold on the Deep Web.

Others agree that it is a bad idea, but say there are times it could be the only feasible idea.

Malik said paying, "should be an absolute last resort."

And Hay said his "security side" would dictate that victims never pay, since that will simply encourage another attack with a larger ransom demand.

But he said his "business side" knows that, "if the business cannot continue to operate without paying the ransom, they'll pay the ransom."

A fresh look at fighting ransomware

If big government and large companies and hospitals can get infected, then everyone can. As the old adage goes, an ounce of prevention is worth a pound of cure.

BY JONATHAN HASSELL

Ransomware is evil, and it continues to prey upon thousands of businesses every year. Most infections are fairly quiet affairs: A small business gets infected, almost always by some employee opening an email attachment he or she mistakes as legitimate but that really contains the payload of a virus. Then several undetected hours later, all of the business' files — at least those the employee had access to, which in a lot of businesses without good security and permissions policies is all of the files — are encrypted, and demands for payment of a ransom in bitcoin are made in exchange for the decryption key.

Of course, secure email use and employee behavior is a problem in businesses of all sizes, and there have been some high-profile ransomware infections. Recently in the news was the attack on the San Francisco Municipal Transportation Agency (SFMTA), or Muni as it is known by Bay Area residents. Muni had to give free trips to all comers over the Thanksgiving weekend while it worked to restore access to its machines. The hacker who infected the utility also claims to have access to 30GB of stolen Muni data; the utility disputes this claim, but it is certainly possible.

If big government and large companies and hospitals can get infected, then everyone can.

I've written about ransomware before, but that was ages ago in internet time. In this piece, I would like to take a fresh look at approaches to combat ransomware. You will note that two of these approaches are predicated on preventing the infection in the first place, because — as the old adage goes — an ounce of prevention is worth a pound of cure. The other approach leaves a bad taste in anyone's mouth, but it is something that is worth discussing: If you have been victimized by ransomware, should you just pay the ransom, or are there other options?

Ransomware ground rules

First, some blanket caveats we should get out of the way.

Your existing antivirus solution is pretty much worthless at detecting ransomware. The ransomware creators have gotten very good at eluding most methods that today's antimalware software uses to identify and quarantine threats. Unfortunately, far too many organizations think slapping a copy of Symantec Endpoint Protection or something similar on all of their workstations will prevent this kind of malware from infecting their network. This is simply not the case. Antivirus solutions are good at eliminating other threats, but they are extremely poor at detecting ransomware.

Backups are the only legitimate way to avoid paying the ransom. According to the Krebs on Security report, this was the mitigation used by San Francisco's Muni. "We have an

information technology team in place that can restore our systems, and that is what they are doing," SFMTA spokesman Paul Rose told the Krebs team a few days after the attack. "Existing backup systems allowed us to get most affected computers up and running this morning, and our information technology team anticipates having the remaining computers functional in the next two days."

I was about to write that backups are the "only foolproof way" to avoid paying the ransom, but that is not the case. You have to regularly and consistently test your backups by restoring them to spare hardware or a virtual machine to make sure they are good — otherwise you have not backed up. If a tree falls in the forest, but there is no one around to hear it, does it make a sound? Similarly, if a backup is made but there's no way to restore it, have you prepared for a disaster? In a word, no.

User education is also key for preventing ransomware. All of the technical solutions in the world will not help if your users still open up "XLS" and "ZIP" attachments that end up being anything but. Blacklisting and spam control can only go so far, and ransomware comes in with such a wide variety of payloads and covers that it can end up being counterproductive to try to ban, say, all ZIP files or all XLS files from coming into your organization over email. Better to train your users to suspect all attachments are bogus, only open those they know are coming and delete anything they are not absolutely sure about before opening — or call you.

Use File Server Resource Manager file screens

One of the more unheralded tools in the Windows Server arsenal is the File Server Resource Manager, or FSRM for short. Using the FSRM, you can develop file screens that monitor the activities on the disk of the file server to look for suspicious activities, notify an administrator that something that may be untoward is happening and then prevent the user from continuing to access those shares. With an FSRM screen like this, an attacker might manage to encrypt a few files, but the screen ought to catch the activity before too much damage is done.

The FSRM design works like this: First, create a file share on your network to act as a honeypot. Regular users would not use the share for anything, but when the ransomware programmatically goes through to attempt to encrypt things, it doesn't know what shares are normally used, so it just encrypts all of the shares and files it can see. If you see activity in this share, you can safely assume it is ransomware, so then you have FSRM send you an email and then fire off a couple of commands to change permissions in order to block that particular user from further network access.

To get started, install the FSRM from Server Manager (it's in the Tools menu), and then, once installed, launch the FSRM console from the Start menu. Configure your email notifications — in the right pane, click Configure Options, click the E-mail Notifications tab, and then enter your SMTP server information. You can send a test email right from that screen to make sure everything works.

Next, create a honeypot file share. Use whatever tool you like for this, but make sure you give the Authenticated Users group (this is anyone with an active logon) full access to this share. You might also want to use a special character to force this share to the top of an alphabetically sorted list to hopefully fool the ransomware into starting there first. For example, to do this in PowerShell, you could use this command:

```
New-SmbShare -Name "$HPImportant-
Files" -Path "C:\ClusterStorage\
Honeypot" -FullAccess "DOMAIN\Authen-
ticated Users"
```

Next, in the right pane, click File Screens, and then click Create File Screen. Pick your honeypot share, and then click Define custom file screen properties. Choose Active screening

under screening type, and then under Maintain file groups, click Create. Call the group "Honeypot files" and then under files to include, use *.* to include all files. Click OK, then check the box beside your new group in the File Groups box. Click over to the next tab, check Send email, and customize the email to be sent if this screen is triggered. Then click over to the Command tab, and then enter the path to PowerShell.exe on your servers in the first box; in the second box, enter the following:

```
-ExecutionPolicy Unrestricted -NoLogo
-Command "&amp;amp; { Get-SmbShare
-Special $false | ForEach-Object {
Block-SmbShareAccess -Name $_.Name
-AccountName '[Source Io Owner]'
-Force } }"
```

That PowerShell command allows the command to execute, looks for the current share that is being triggered and then blocks access via SMB permissions for that user.

Once you get the machine cleaned up for the user, you'll want to restore permissions to the honeypot so that your canary in the coal mine can work again. You could do that in PowerShell like so:

```
Get-SmbShare -Special $false |
ForEach-Object { Unblock-SmbShareAc-
cess -Name $_.Name -AccountName 'use-
rinquestion' -Force }
```

Use secured offline backup

The ransomware we are seeing these days is much more sophisticated than the early variants that infected only mapped drives with assigned drive letters and did not know how to navigate Universal Naming Convention (UNC) shares and Windows Distributed File System (DFS) paths. The newest strains of Cryptolocker and its cousins not only traverse the network, they infect the "previous versions," or shadow copies, that Windows makes of files. (And if they don't infect them, they instead turn off the volume shadow copy service and then delete the previous versions already present on the disk, making this line of defense no longer suitable to prevent ransomware attacks.) And it is even possible for unencrypted backups to also be infected and encrypted, rendering them absolutely worthless in any effort to avoid paying the ransom.

If you back up to a location that is still connected to the network, your backups are at risk — there is no way around it. This is typically why active backup strategies involving rotating hard drives are best when it comes to defending from these types of threats. Unfortunately, many businesses now rely solely on online backup strategies, backing up to a service in the cloud that by design must always have a network connection — so it is a very simple technical task on the part of the ransomware to encrypt those backups too.

Some tips for effective backups:

- Add an offline backup as part of your strategy. Back up at least once weekly, and more often if your needs dictate, to tape or spinning media and then immediately disconnect that media from your network and store it somewhere safe.
- For online backups, ensure that only the right users have permissions to access files and file shares of the files to back up as well as the location where the online backup files are stored.

Should you just pay the ransom?

As distasteful as it may be to reward this kind of hacking, there are some businesses without recent accessible backups that have been hit by Cryptolocker and its relatives that simply have no choice but to take a chance and pay the ransom.

How do you know the hackers will make good on their attempts? To date, there have only been a couple of instances when bitcoins were

transferred but the crackers did not make good on releasing decryption keys. To do otherwise would be tremendously short-sighted: There is no profit motive in simply encrypting peoples' files, only the small amount of "satisfaction" these crackers would get from causing general mayhem. The profit comes when users trust in the process enough that paying the ransom actually gets their files back.

Word spreads, more computers are infected, more files are encrypted and there are more opportunities to get ransom payments. If the crackers were to stop honoring the ransom payment, no one would have an incentive to pay, and this undeniably strong black market revenue source would dry up almost overnight.

All of this is to say yes, sometimes your only option is to pay up. But a few tips:

Before you pay, please look at the Bleeping Computer forums to see if others in the community have cracked the encryption algorithm of the particular ransomware variant you were unlucky enough to get. Hundreds of keys and additional assistance are available at this invaluable resource.

Don't be afraid to negotiate with the hacker. Yes, he or she has leverage over you, but you also have leverage — you have the money. There are many reports, especially from mid-size and large businesses, of reducing the actual amount of ransom paid by up to 75 percent over the original ransom demand.

Attempt to hide your own identity as much as possible. While most ransomware variants currently do not change the amount of ransom demanded based on the number of related computers they detect are infected, some do, and this is clearly an area where revenue for the hackers could grow.

Try not to let on that your whole business is shut down. Avoid mentioning that "n" people will be out of work unless you get your files back. Do not mention what type of data is in the files they have encrypted. Say only what you must, and nothing more, to avoid escalation in ransom demands.

Most victims able to thwart attacks, report says

In only 3 percent of cases were companies unable to restore the encrypted files, according to the report.

BY MARIA KOROLOV

The vast majority of companies hit by ransomware attacks were able to stop the attacks by either preventing the malware from getting to their files, by successfully decrypting the files, or by restoring the files from backups, according to a report released in November, 2016 by SentinelOne.

In a Vanson Bourne survey of 500 cybersecurity decision makers conducted in October, 2016, 48 percent of respondents said their organizations had been hit by at least one ransomware attack in the last 12 months, with the average victim hit six times.

In 27 percent of the cases, the attacker couldn't encrypt any files. In 45 of the attacks, some files were encrypted, but the companies were able to decrypt them on their own. In 25 percent of the cases, the company was able to replace the encrypted files from backups.

Only in 3 percent of the cases were the companies unable to restore the encrypted files.

Paying the ransom usually solved the problem, but the attackers often came back to ask for more money first, said Jeremiah Grossman, chief of security strategy at SentinelOne, which sponsored the report.

And for companies, the amounts the attackers asked for were significantly higher than for home computers.

Grossman warned that the sample size was very small, but of the 10 respondents who answered the question about how much they paid, most said that the total was between $37,000 and $49,000.

By comparison, home users typically spend between $500 and $2,000 on ransomware payments, based on other surveys, he said.

But attackers typically ask for the lower amounts in indiscriminate, widespread attacks, he said.

"Now the attacks seem to be targeted," he said. "The bad guys are going after more money."

The ransomware is also getting more sophisticated.

In some ransomware, the key used to encrypt the files is the same as the key that decrypts them, and is embedded in the malware. Another mistake that hackers sometimes make is using the same key for all their ransomware infections, so once one victim pays and gets the key, all other victims can then use the key to decrypt their files.

"I personally think that era, the era of unlockers, is short lived," Grossman said. "Some of the bad guys are still in amateur mode but we can expect the malware families to grow in sophistication and effectiveness. The bad guys will move almost universally to asynchronous encryption."

That's where one key is used to encrypt the files, and a different key is used to decrypt them.

More of the ransomware will also use different keys for each victim, he added.

"Every time you pay a ransom, you embolden the bad guys and give them resources," he said.

"So you'll expect to see more ransomware, and more research and development going into ransomware to make it more effective."

Last summer, SentinelOne, which makes endpoint protection products, offered a ransomware guarantee of up to $1 million per enterprise — and $1,000 per infected endpoint — if the ransomware gets past their security product.

But the $1,000 amount was based on earlier data, mostly of home user infections, Grossman said.

That amount might be raised, he said, since attackers are asking for higher amounts from corporate victims.

So far, he added, SentinelOne hasn't had to make any payouts to its customers.

"It takes time to explain it to customers," he added. "We expect to have some payouts in the future — there just hasn't been enough time for those to come in yet."

Why you shouldn't pay the fee

Criminals are making a lot of money with ransomware attacks because they are playing a game of psychological warfare with their victims. The bad guys know that no one wants to look like a fool.

BY KACY ZURKUS

While most of the decision makers would likely prefer to hear a simple yes or no when asking if they should pay, nothing in security is simple. By and large, the position of many leaders in the industry is that the ideal situation is not to pay.

Security experts across the industry would like to see all enterprises, large and small, be prepared for a hit so that they can recover their data without paying a ransomware fee. The question of whether to pay the fee is tricky, though, as sometimes organizations are left with no other options.

When asked whether companies should ever pay a ransomware fee, Ryan Manship, security practice director at RedTeam Security said, "The first thing about ransomware is that it's in many ways like terrorism. The U.S. has a policy not to negotiate with terrorists. Where does that come from? Why does it exist? The reality is, you can't trust the bad guys. You can't trust them to do what they say they are going to do, which is to give back access to your data."

True, there is the issue of being able to trust that this is a single payment that will result in the return of data as promised, but enterprises that are hit with ransomware also experience the hard fact that a hit can make your most critical information inaccessible and in some cases not recoverable at all.

"Some people might argue that paying is a viable option at that point," Manship said. In paying, though, they also have to consider whether they can trust that the bad guys are going to keep their word. Certainly, this act of holding data hostage could become a continuous cycle.

Manship said, "There is no evidence that decrypting data means they are out of your system. Are they going to give you the key? How many times are they going to try to extort money out of you until they laugh and walk away and you are out of luck?"

Determining whether or not to pay is a call much easier made in the hypothetical. Hospitals have been frequent targets of ransomware attacks of late, which presents a precarious situation for those who have to weigh out the risks and rewards of recovery. One extreme consequence of being hit by ransomware for the healthcare industry is that downtime could directly impact patient health.

Though it's likely little help to say that every situation is different, Manship said, "I don't presume to be able to predict the right action when people's lives are on the line. I can't presume to suggest the right course of action. Still though, I have to suggest that we don't recommend that

course of action because it sets a precedent and that's a dangerous precedent to set."

No industry wants to set the precedent that they are the most lucrative target, which is why having a conversation in strict black and white terms of paying or not paying isn't feasible. "Every organization is different," said Sean Mason, director, threat management and incident response, Cisco Security Services.

Government agencies and private enterprises have two very different ways of looking at the world. Mason said, "For government agencies ransomware is terrorism versus the private enterprise that has an obligation to their shareholders and customers."

Whether to pay a ransomware fee really depends on what type of organization they are because if an attacker can come in and essentially shut them down, that is a significant impact with costly repercussions. Understanding the impact of what has happened to the organization is important and ought not to be clouded by fear.

Many do share the concerns of Mike Hanley, director of Duo Labs at Duo Security who spoke about the continued attacks on hospitals. Hanley said that these attacks can directly impact patient health, but Mason isn't as convinced that there is a correlation.

"It's easy to say that a hospital got hit and patient lives are at risk, but that is not necessarily the case. It can be down the road, but I have not read about or seen one where patient lives were at risk," said Mason.

"I think there are a number of cases where they should pay, and I say that unfortunately. If there is an impact to human life, that's a no brainer. You pay the ransom," Mason said.

Criminals prey on the fear of their victims whether the ransomware impacts patient health or shareholder profit. They know that every minute without access translates to some sort of loss, and they rely on the hope that their victims will pay, which is why paying should be a last resort.

Taking a firm stand that nobody will ever pay is not realistic or even feasible, as proven by the fact that ransomware is a viable business model for criminals. "It works," said Mason, "and to unilaterally say we won't pay again is not in the realm of possibility."

Instead, enterprises should prepare themselves for an imminent attack so that they are well placed to recover and move on. Lance James, chief scientist at Flashpoint, noted that ransomware is a symptom of a bigger problem.

"There is malware that comes in before the ransomware drops in, like Pony, Dridex, or other information stealing malware, so those systems are already infected and they are stealing other data as well," James said.

Many enterprises should be able to quickly recover without having to pay. "Paying is ill advised. There is already a security flaw if they are getting in the door. Hopefully those who have already been attacked will focus on thinking about the ransomware hit as a problem in their environment," James said.

For those who have yet to be victims, treat a potential ransomware attack as they would prepare for a server crashing. James said, "They need to be thinking about which files matter, and if those are captured, do they have another way to get them." Have redundant copies of every file, shadow copies, and take that data and keep it off the network and safely away from the ransomware.

Criminals are making a lot of money with ransomware attacks because they are playing a game of psychological warfare with their victims. Rather than pay the fee to them, pay in advance to defend at the endpoint, or pay a trusted forensics team to help with recovery. The bad guys know that no one wants to look like a fool, which is why, James said, many people have actually lied about being hit and paid the fee quietly.

Rather than succumb to the psychological coercion, James said, "There needs to be more situational awareness. It's OK to get hit. It's

OK to talk about it, and it's OK to have a plan and to not hide it. The alternative is that they are creating a hot spot for ransomware getting worse when criminals realize what else they can make people do, whether that means blackmail or causing the company harm."

Organizations need to remember that just because they pay the ransom, that doesn't guarantee they will get their data unlocked or unlocked with no further impact. They are, after all, dealing with criminals.

Resources

Sponsored by KnowBe4 Human error. Conquered.

MANUAL

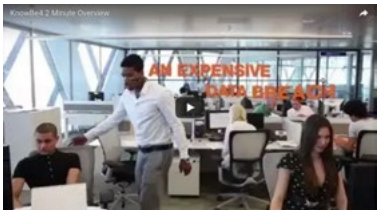
Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware. **DOWNLOAD**

FREE TOOL

Ransomware Simulator

KnowBe4's Ransomware Simulator "RanSim" gives you a quick look at the effectiveness of your existing network protection. RanSim will simulate 10 ransomware infection scenarios and show you if a workstation is vulnerable to infection. **DOWNLOAD**



VIDEO

Are You Protected Against the Weakest Link in Network Security?

Watch this 2-minute video and learn how you can keep your users on their toes with security top of mind. **DOWNLOAD**

FREE TOOL

Phishing Security Test

91% of successful data breaches started with a spear phishing attack. Find out what percentage of your employees are Phish-prone™ with your free phishing security test. **DOWNLOAD**

FREE TOOL

Domain Spoof Test

Would you like to know if hackers can spoof your domain? KnowBe4 can help you find out if this is the case with our Domain Spoof Test. It's quick, easy and often a shocking discovery. **DOWNLOAD**